

## INDEX

<b>Access Cards</b>	Departing Workforce Members Access Cards/Keys	Ch. 4, Sec. III.B.3 Ch. 6, Sec. IV.B
<b>Access Coordinator(s)</b>	Duties  Risk Management Audit	Ch. 4, Sec. II.C. and D Ch. 4, Sec. III.C Ch. 4, Sec. VII Ch. 8, Sec. IV.B Ch. 8, Sec. V
<b>Access Procedures</b>	Network DMH Applications Terminating/Suspending Emergency Modifying Sanction Restarting Non-DMH Workforce Reviewing	Ch. 4, Sec. II Ch. 4, Sec. II.D Ch. 4, Sec. III Ch. 4, Sec. III.C Ch. 4, Sec. IV Ch. 4, Sec. IV.A.2 Ch. 4, Sec. V Ch. 4, Sec. VI Ch. 4, Sec. VII
<b>Activity Review</b>	Risk Management	Ch. 8, Sec. IV.A
<b>Agreements:</b> • <b>DMH IT User Acknowledgment Form</b>  • <b>EOHHS Remote Access Agreement</b>  • <b>EHS Mobile Device Policy/Agreement</b>	Training Requirement for Access to: Network DMH Applications  VPN Access Non-DMH Workforce  Compliance	Ch. 4, Sec. II.B Ch. 4, Sec. D.3  Ch. 4, Sec. II.F Ch. 4, Sec. VI  Ch. 6, Sec. VII.C
<b>Anti-Virus Software</b>		Ch. 6, Sec. VII.B
<b>Application Owner</b>	EPHI Registration Duties Criticality Levels Access Procedures Risk Management Audit System Specific Business Continuity and Disaster Recovery Plans	Ch. 3, Sec. II Ch. 3, Sec. II.D Ch. 4, Sec. II.D Ch. 8, Sec. IV.B Ch. 8, Sec. V Ch. 9, Sec. III.C
<b>Area Director, Appointment of Area Information Security Coordinator</b>		Ch. 1, Sec. II.B

<b>Assistant Chief Information Officer (ACIO)</b>	Acquisition of Electronic Information Recourses Installation of Software Restriction of Use Risk Mitigation System Specific Business Continuity and Disaster Recovery Plans	Ch. 3, Sec. III  Ch. 5, Sec. V Ch. 7, Sec. II.4 Ch. 8, Sec. VIII Ch. 9, Sec. III.C. and E
<b>Audits</b>	Systems and Databases Application Owners and Access Coordinators System Specific Business Continuity and Disaster Recovery Plans	Ch. 8, Sec. IV.B Ch. 8, Sec. V  Ch. 9, Sec. III.E
<b>Back-Up</b>	Relocation of Non-Portable Information Resource Content of Specific Plan	Ch. 6, Sec. X.A  Ch. 9, Sec. III.C.2.b.
<b>Business Continuity and Disaster Recovery Plan</b> (See also Specific Plan)	Criticality Levels Responsibility Contents Documentation	Ch. 3, Sec. II.D Ch. 9, Sec. III.A Ch. 9, Sec. III.B Ch. 9, Sec. III.D
<b>Chain Letters</b>		Ch. 7, Sec. II.9
<b>Change of Position within DMH</b>		Ch. 4, Sec. IV.A.1
<b>Commonwealth Workstations at Non-DMH Locations</b>		Ch. 6, Sec. VII.B.7
<b>Complaints</b>	DMH ISO Responsibilities Contact Information Free from Intimidation or Retaliation Reporting to DMH Reviews	Ch. 1, Sec. II.A and IV Ch. 1, Sec. VII Ch. 1, Sec. VIII  Ch. 2, Sec. III.F Ch. 8, Sec. IV.C.
<b>Compliance, With Handbook</b>	Required Sanctions for Non-Compliance Risk Management	Ch. 1, Sec. III Ch. 1, Sec. VI  Ch. 8, Sec. III
<b>Computer Training Rooms</b>		Ch. 6., Sec. IV.A.6
<b>Confidentiality</b>	HIPAA Standards DMH Data	Ch. 1, Sec. I.B Ch. 5, Sec. III.B
<b>Confidentiality Notice, for Emails</b>		Ch. 7, Sec. III.C.2

<b>Continuity of Operations Plan (COOP)</b>		Ch. 9, Sec. II.B. and C
<b>Contract Language</b>	Required for Non-DMH Workforce Member to access DMH Network	Ch. 4, Sec. VI
<b>Copyright, Comply With</b>		Ch. 5, Sec. II
<b>Criticality Levels for IT Systems and Databases</b>	Establish Levels Business Continuity and Disaster Recovery Plan Specific Plan	Ch. 3, Sec. II.D Ch. 9, Sec. III.B  Ch. 9, Sec. III.C
<b>Data Centers</b>		Ch. 6, Sec. IV.A.4
<b>Data Confidentiality</b>		Ch. 5, Sec. III.B
<b>Data Transmission</b>		Ch. 5, Sec. IV
<b>Data Back-Up Plans</b>		Ch. 9, Sec. III.C.2.b
<b>Deleting / Disposing of EPHI</b>		Ch. 6, Sec. VIII
<b>Departing Workforce Members</b>	General Actions to be Taken	Ch. 4, Sec. III Ch. 4, Sec. III.B
<b>Device(s)</b>		Ch. 6, Sec. VII.C
<b>Digital Media</b>		Ch. 6, Sec. VII.C
<b>Director of Emergency Management</b>	Duties	Ch.1, Sec. V.A.1 Ch. 9, Sec. II. B Ch. 9, Sec. III. A , and D
<b>DMH Application (See Access Procedures)</b>		
<b>DMH Employees</b>	Duties	Ch. 1, Sec. III
<b>DMH Information Security Officer (DMH ISO)</b>	Duties Complaints Contact Information Information Security Incidents EPHI Systems/Databases Registration Approval of Access Procedure Security Plans Monitoring Activities Audits Evaluation Risk Mitigation Contingency Plans	Ch. 1, Sec. II, IV, and V Ch. 1, Sec. VII Ch. 1, Sec. VII Ch. 2, Sec. IV and VIII  Ch. 3, Sec. II  Ch. 4, Sec. II.D  Ch. 6, Sec. II.A. 4 and 5 Ch. 8, Sec. IV Ch. 8, Sec. V Ch. 8, Sec. VII Ch. 8, Sec. VIII Ch. 9, Sec. III.C.2.c. and Sec. III.D. and E
<b>DMH Internal Controls Officer</b>		Ch. 2, Sec. VI

<b>DMH IT User Acknowledgment Form</b>	Training Requirement for Access to: Network DMH Applications	Ch. 4, Sec. II.B Ch. 4, Sec. II.D.3
<b>DMH Learning and Development Office</b>	Training Computer Training Rooms	Ch. 1, Sec. V.A Ch. 6, Sec. IV.A.6
<b>DMH Managers</b>	Duties: <ul style="list-style-type: none"> <li>• General</li> <li>• Monitoring</li> </ul> May Restrict Access in Emergency Must Approve Access for Non-DMH Workforce May Restrict Use of: <ul style="list-style-type: none"> <li>• Workstation</li> <li>• Email</li> </ul> May Approve Use of: <ul style="list-style-type: none"> <li>• Personal Device</li> <li>• Digital Media</li> </ul>	Ch. 1, Sec. III.A Ch. 5, Sec. II.C. Ch. 4, Sec. III.C  Ch. 4, Sec. VI  Ch. 6, Sec. VII.B.8 Ch. 7, Sec. II.4  Ch. 6, Sec. VII.A Ch. 6, Sec. VII.C.2
<b>DMH Ownership, of Electronic Information Resources, Emails and Data</b>		Ch. 5, Sec. III
<b>DMH Privacy Officer</b>	Verification of Designated Record Set Business Associate Language	Ch. 3, Sec. II.C  Ch. 4, Sec. VI.B.7
<b>DMH Standard Issue Software Suite</b>		Ch. 5, Sec. V
<b>DMH Supervisor</b>	Duties: <ul style="list-style-type: none"> <li>• General</li> <li>• Monitoring</li> </ul> Sanctions of Non-Employees Access, Network Access, DMH Applications Minimum Necessary VPN Requests Departing Workforce Member, Actions to be Taken Access, Modification Access, Restarting	Ch. 1, Sec. III.A Ch. 5, Sec. II.C Ch. 1, Sec. VI  Ch. 4, Sec. II Ch. 4, Sec. II.D Ch. 4, Sec. II.E Ch. 4, Sec. II.F Ch. 4, Sec. III.B  Ch. 4, Sec. IV.B Ch. 4, Sec. V
<b>Documentation Reviews</b>		Ch. 8, Sec. IV.D

<b>EHS Information Technology (EHS IT)</b>	Prevention of Incidents Access Procedures Installation of Software Issuance of laptop Return of Electronic Information Resource System Specific Business Continuity and Disaster Recovery Plans and Back-Ups	Ch. 2, Sec. V Ch. 4 Ch. 5, Sec. V Ch. 6, Sec. VII.B.10 Ch. 6, Sec. IX  Ch. 9., Sec. III.C
<b>EHS Mobile Device Policy/Agreement</b>	Compliance	Ch. 6, Sec. VII.C
<b>EHS Security Office</b>		Ch. 2, Sec. VIII
<b>EHS Support Services (also known as the Help Desk)</b>	Reporting Incidents Access	Ch. 2, Sec. III.C Ch. 4
<b>Electronic Protected Health Information (EPHI)</b>	Registration of EPHI Systems/Databases Access Data Confidentiality Electronic Transmission Safeguards Storage Regular Disposition Moving Non-Portable Information Resource Email Containing Systems and Databases Reviews and Audits	Ch. 3  Ch. 4 Ch. 5, Sec. III.B Ch. 5, Sec. IV Ch. 6, Sec. VII.B Ch. 6, Sec. VII.C Ch. 6, Sec. VIII Ch. 6, Sec. X  Ch. 7 Ch. 8, Sec. IV.B
<b>Electronic Transmissions</b>		Ch. 5, Sec. IV
<b>Email</b>	Use in General Public Records Restrict Use Containing PHI Misdirected Remote Access	Ch. 7, Sec. II Ch. 7, Sec. II.2 Ch. 7, Sec. II.4 Ch. 7, Sec. III Ch. 7, Sec. III.D Ch. 7, Sec. IV
<b>Emergency Planning</b>	DMH infrastructure	Ch. 9, Sec. II
<b>Emergency suspension of access to Information Resources</b>		Ch. 4, Sec. III.C
<b>Entrances, to DMH Locations</b>		Ch. 6, Sec. III
<b>Environmental Controls</b>		Ch 6, Sec. IV.A.7

<b>EOHHS Remote Access Agreement</b>	VPN Access Non-DMH Workforce	Ch. 4, Sec. II.F Ch. 4, Sec. VI
<b>EPHI System/Database</b>	Registration Registration Form Establish Criticality Levels	Ch. 3, Sec. II Ch. 3, Sec. II.B.2 Ch. 3, Sec. II.D
<b>Evaluation of Security Safeguards</b>		Ch. 8, Sec. VII
<b>Exe Files</b>		Ch. 5, Sec. II.A.9
<b>Fair Information Practices Act</b>		Ch. 5, Sec. III.A.1
<b>Forms:</b> <ul style="list-style-type: none"> <li>• <b>EPHI System/Database Registration Form</b></li> <li>• <b>HRD Forms</b></li> <li>• <b>DMH Application Request Form</b></li> <li>• <b>DMH Exit Checklist</b></li> <li>• <b>MHIS User Access and Provider Request Form</b></li> <li>• <b>Security Plan Form</b></li> <li>• <b>Security Walk Through Job Aid</b></li> </ul>		Ch. 3  Ch. 4 Ch. 4  Ch. 4 Ch. 4  Ch. 6 Ch. 6
<b>Global Address List (GAL)</b>		Ch. 7, Sec. III.C.1
<b>Hardware</b>	Connected by IT only	Ch. 5, Sec. II.A.5.c.
<b>Health Insurance Portability and Accountability Act of 1996 (HIPAA)</b>		Introduction
<b>HIPAA Security Rule</b>	Compliance with	Ch. 1, Sec. I
<b>HIPAA Security Standards</b>		Ch. 1, Sec. I.B
<b>Identification Badges</b>		Ch. 6, Sec. V
<b>Incident</b> (See Information Security Incident)		
<b>Information Resources</b>	Acquisition Use Monitoring Ownership Electronic Transmissions Software Restrictions	Ch. 3, Sec. III Ch. 5 Ch. 5, Sec. II.C Ch. 5, Sec. III Ch. 5, Sec. IV Ch. 5, Sec. V

	Physical and Technical Security Security Plans Located at Non-DMH Locations Returning Resource when use is completed	Ch. 6  Ch. 6, Sec. II Ch. 6, Sec. VII.B.7  Ch. 6, Sec. IX
<b>Information Resources (IR) Policies and Procedures</b>	General Rules of Use	Ch. 5, Sec. II
<b>Information Security Coordinators</b>	Appointment/duties Meetings Assessments of Trainings Documentation Reviews	Ch. 1, Sec. II.B Ch. 1, Sec. II.B Ch. 1, Sec. V.A.2 Ch. 8, Sec. IV.D
<b>Information Security Incident</b>	Definition Reporting Log Response Prevention Reviews	Ch. 2, Sec. II Ch. 2, Sec. III Ch. 2, Sec. III.D Ch. 2, Sec. IV Ch. 2, Sec. V Ch. 2, Sec. VIII
<b>Internet Use</b>		Ch. 5, Sec. II.B
<b>IT System or Database</b>	Establish Criticality Levels Business Continuity and Disaster Recovery Plan Specific Plan	Ch. 3, Sec. II.D Ch. 9, Sec. III. B  Ch. 9, Sec. III. C
<b>Key Control Plan</b>		Ch. 6, Sec. IV.B
<b>Laptops</b> (See Workstations)		
<b>Leave DMH</b>	Departing Workforce Member	Ch. 4, Sec. III
<b>Log Off</b>	Safeguards, Network Safeguards, Devices	Ch. 6, Sec. VII.B.2 Ch. 6, Sec. VII.C.4.c
<b>Logs</b>	Information Security Incident Visitors	Ch. 2, Sec. III.D  Ch. 6, Sec. V.B
<b>Maintenance and Repairs of DMH Electronic Information Resources</b>		Ch. 6, Sec. VI
<b>Massachusetts Statewide Record Retention Schedule</b>	Disposition of EPHI Disposition of Email Maintenance of Security Plan	Ch. 6, Sec. VIII and IX Ch. 7, Sec. II.3 Ch. 6, Sec. II.A.6
<b>Misdirected Emails</b>		Ch. 7, Sec. III.D
<b>Monitoring</b>	Use	Ch. 5, Sec. II.C

	Activities, Systems and Databases Advancements Business Continuity and Disaster Recovery Plan	Ch. 8, Sec. IV  Ch. 8, Sec. II Ch. 9, Sec. III.B
<b>Moving Non-Portable Information Resource with EPHI</b>		Ch. 6, Sec. X
<b>Network</b>	Access Non-DMH Workforce Access Use Wire Closets Safeguards and Compliance	Ch. 4 Ch. 4, Sec. VI  Ch. 5 Ch. 6, Sec. IV.A.5 Ch. 6, Sec. VII
<b>Network Monitoring</b>		Ch. 2, Sec. V
<b>Non-Portable Information Resources</b>	Moving	Ch. 6, Sec. X
<b>OIM Director, Designation of OIM Security Coordinator</b>		Ch. 1, Sec. II.B
<b>Outlook Web Access (OWA)</b>		Ch. 7, Sec. IV
<b>Ownership of Information Resources and Data</b>		Ch. 5, Sec. III
<b>Passwords</b>	Access Control Workforce Use	Ch. 1, Sec. III.B.3 Ch. 5, Sec. II.C.2
<b>Person in Charge</b>	Responsible for Security Plan Access Card/Key Control Plan System Specific Business Continuity and Disaster Recovery Plans	Ch. 6, Sec. II.A  Ch. 6, Sec. IV.B  Ch. 9, Sec. III.C.2.a
<b>Personal Devices</b>	Subject to Seizure Use Prohibited	Ch. 2, Sec. VII Ch. 6, Sec. VII.A
<b>Physical Transportation</b>		Ch. 6, Sec. VII
<b>Policies, Information Security</b>		Introduction Ch. 1, Sec. IV
<b>Political Use</b>		Ch. 7, Sec. II.9
<b>Public Record</b>		Ch. 5, Sec. III.A.1 Ch. 7 Sec. II.2
<b>Public Service Announcement</b>		Ch. 7, Sec. II. 5



<b>Questions, Concerns Regarding Security</b>		Ch. 1, Sec. VII
<b>Reasonable Accommodation</b>		Ch. 8, Sec. III.B
<b>Recommendations, By Workforce Members</b>		Ch. 1, Sec. IV.B
<b>Record Retention</b>	Security Plan EPHI Returning Resource when use is completed Email Documentation	Ch. 6, Sec. II.A.6 Ch. 6, Sec. VIII Ch. 6, Sec. IX  Ch. 7, Sec. II.3 Ch. 8, Attachment A
<b>Registration EPHI System/Database</b>		Ch. 3, Sec. II
<b>Re-Imaging</b>		Ch. 6, Sec. VII.B.10
<b>Remote Access</b>	Network (VPN) Non-DMH Workforce Personal Device Email only	Ch. 4, Sec. II.F Ch. 4, Sec. VI Ch. 6, Sec. VII.A Ch. 7, Sec. IV
<b>Repairs</b>		Ch. 6, Sec. VI
<b>Reporting an Information Security Incident</b>		Ch. 2, Sec. III
<b>Restricted Areas</b>		Ch. 6, Sec. IV
<b>Retaliation, Free From</b>		Ch. 1, Sec. VIII
<b>Return of Information Resources, to EHS IT</b>		Ch. 6, Sec. IX
<b>Reviews</b>	Information Security Incidents EPHI Systems/Databases: <ul style="list-style-type: none"> <li>• Inventory</li> <li>• DRS</li> </ul> Security Plans Monitoring Activities Documentation	Ch. 2, Sec. IV and VIII  Ch. 3, Sec. II.A Ch. 3, Sec. II.C Ch. 6, Sec. II Ch. 8, Sec. IV Ch. 8, Sec. IV.D
<b>Risk Analysis</b>		Ch. 8, Sec. II
<b>Risk Management</b>		Ch. 8, Sec. III and IV
<b>Sanctions for Non Compliance</b>		Ch. 1, Sec. VI
<b>Secure File Email Delivery System (SFED)</b>		Ch. 7, Sec. III
<b>Secure File Transfer Protocol (SFTP)</b>		Ch. 5, Sec. IV.A
<b>Security Alerts</b>		Ch. 1, Sec. V.B
<b>Security Personnel</b>		Ch. 1, Sec. II

<b>Security Plans for Information Resources</b>		Ch. 6, Sec. II
<b>Security Standards</b>		Ch. 1, Sec. I.B
<b>Security Testing</b>		Ch. 9, Sec. III Ch. 9, Sec. IV.E
<b>Sensitive Information</b>	Confidentiality Security Plans Safeguards/Storage	Ch. 5, Sec. III.B Ch. 6, Sec. II Ch. 6, Sec. VII
<b>Separation of Duties</b>		Ch. 1, Sec. IX
<b>Software as a Service (SaaS)</b>	Business Continuity and Disaster Recovery Plan Specific Plans	Ch. 9, Sec. II.B.2  Ch. 9, Sec. III.C
<b>Software</b>	General Rules Restriction on Installation Anti-Virus	Ch. 5, Sec. II.A Ch. 5, Sec. V Ch. 6, Sec. VII.B
<b>Specific Plan (System Specific Business Continuity and Disaster Recovery Plans)</b>	Inclusion in Business Continuity and Disaster Recovery Plan Responsibility Contents Documentation Testing and Audits	Ch. 9, Sec. III.B.9  Ch. 9, Sec. III.C.2 Ch. 9, Sec. III.C.2.b. Ch. 9, Sec. III.D Ch. 9, Sec. III.E
<b>Statewide Record Retention Schedule</b> (See Massachusetts Statewide Record Retention Schedule)		
<b>Storage</b>	Sensitive Information, including EPHI	Ch. 6, Sec. VII.C.3
<b>Suspended from Work</b>		Ch. 4, Sec. III
<b>Suspicious Activities, Duty to Report</b>		Ch. 6, Sec. IV.C
<b>System Reviews</b>		Ch. 8, Sec. IV
<b>Telework(ing)</b>		Ch. 6, Sec. VII
<b>Terminating Access</b>		Ch. 4, Sec. III
<b>Terminating DMH Employment</b>		Ch. 4, Sec. III
<b>Testing</b>	Business Continuity and Disaster Recovery Plan Specific Plans Contingency Plans	Ch. 9, Sec. III  Ch. 9, Sec. III.C Ch. 9, Sec. III.E
<b>Training</b>	DMH Workforce Training and Updates Documentation	Ch. 1, Sec. III.B and V Ch. 1, Sec. V Ch. 1, Sec. V

	Requirement for Access System Specific Business Continuity and Disaster Recovery Plans	Ch. 4, Sec. II.B Ch. 9, Sec. III.C.2.b.
<b>Transfer within DMH</b>	Modifying Access	Ch. 4, Sec. IV
<b>Transporting Data, Physical</b>		Ch 6, Sec. VII and X
<b>Updates</b>	Alerts and Notices DMH ISO to General Counsel	Ch. 1, Sec. V.B Ch. 8, Sec. VI
<b>Use/User</b>	Information Resource Email	Ch. 5, Sec. II Ch. 7
<b>Users Expectation of Privacy, None</b>		Ch. 5, Sec. III. A.
<b>Virtual Private Network (VPN)</b>		Ch. 4, Sec. II.F
<b>Virus Protection Software</b>		Ch. 6, Sec. VII.B
<b>Visitor Log</b>		Ch. 6, Sec. V.B.
<b>Visitors' Badges</b>		Ch. 6, Sec. V.B
<b>Waiver</b>	Reasonable Accommodation	Ch. 8, Sec. III.B
<b>Wire Closets</b>		Ch. 6, Sec. IV.A.5
<b>Workforce/ Workforce Members</b>	Responsibilities Security Recommendations Training and Updates Sanctions for Non-Compliance Duty to Report Duty to Cooperate Identification Badges	Ch. 1, Sec. III Ch. 1, Sec. IV  Ch. 1, Sec. V Ch. 1, Sec. VI  Ch. 2, Sec. III Ch. 2, Sec. VI Ch. 6, Sec. V.A
<b>Workstation</b>	Departing Workforce Member Use Monitoring Restricted Areas Safeguards Returning Resource when use is completed Audits	Ch. 4, Sec. III  Ch. 5, Sec. II Ch. 5, Sec. II.C Ch. 6, Sec. IV Ch. 6, Sec. VII Ch. 6, Sec. IX  Ch. 8, Sec. IV.B and V